BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND

AIR FORCE INSTRUCTION 10-1101

AIR FORCE MATERIEL COMMAND
Supplement 1

1 November 2002

Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFMC WWW site at: https://www.afmc-mil.wpafb.af.mil/pdl/

OPR: HQ AFMC/SFXP (Marlene K. Meyer) Certified by: HQ AFMC/SF (Col Leroy L. Walters)
Supersedes AFI 10-1101/AFMCS1, 25 Feb 98 Pages: 5
Distribution: F

This instruction supplements AFI 10-110, *Operations Security*. It explains program management and unique OPSEC requirements in Air Force Materiel Command. This instruction requires the collection and maintenance of information protected by the Privacy Act of 1974. The authority to collect and maintain the data prescribed in this instruction is 10 U.S.C. 8013. This supplement does not apply to the Air National Guard or US Air Force Reserve unit or members.

SUMMARY OF REVISIONS

This supplement is substantially revised and must be completely reviewed. It aligns its guidance with the revised Air Force Instruction 10-1101, 31 May 2001. Revision changes verbiage in DD Form 254, **DoD Contract Classification Specification**, reference to OPSEC requirements in contracts, adds requirement for contracting activities to provide critical information lists to contractors, adds requirement for vulnerability assessments in areas visited by foreign nationals, adds website for Interagency OPSEC Support Staff (IOSS) products, adds date for submission of annual OPSEC report, adds timeframe for HQ AFMC/SFSP OPSEC staff assistance visits (SAVs), and adds the requirement for AFMC units tenant on other MAJCOM installations to participate in the host activity's OPSEC program. A revision is shown by a bar (|).

AFI 10-1101, 31 May 2001, is supplemented as follows:

1.3.1. OPSEC is a key component of Information Operations/Warfare (IO/IW). Coordination with other elements of IO/IW such as Military Deception, Intelligence, and Information Assurance is critical to gain the maximum synergy with increasingly limited resources and the real threat of technology transfer. In today's free-flowing information-based society there are many channels of information easily accessible by potential adversaries. The active use of the internet and information systems to transmit military defense information is a prime example. Factor increasing internet use, web sites, and telephone usage into the organization's overall OPSEC posture. Awareness and continued training are key to successfully protecting critical information (CI) and guarding against its exploitation.

2.2.1. AFMC Product, Logistics, Test Center, site, and subordinate unit OPSEC Program Managers (PMs) will develop and distribute commander approved CI lists within their respective organizations. OPSEC PMs review CI, OPSEC indicators, and associated protective measures annually to ensure relevancy to current mission, activities, and procedures and validate the need for continued protection.

2.2.4. AFMC organizations must consider OPSEC when issuing contracts for both classified and unclassified programs. When an OPSEC requirement is included in a classified contract, indicate "yes" in block 11j of the DD Form 254. In Item 14, include a statement referencing OPSEC requirements in the contract and indicate that the CIs will be provided to the contractor under separate cover and updated as required. All new unclassified contracts that require on-base performance will include a provision that contractors must participate in the installation's OPSEC program. Responsible organizational OPSEC PMs will provide contracting activities with lists of the center or site CI. Direct questions regarding OPSEC requirements for contracts including CI to the center or site OPSEC PM.

2.3.1. Contact the local Air Force Office of Special Investigations (AFOSI) Detachment and the servicing Intel Office to receive current intelligence collection threat information for individual systems, programs, or facilities.

2.6.2.1. AFMC Product, Logistics, Test Center, and site OPSEC PMs will ensure they or their subordinate unit OPSEC PMs conduct an OPSEC vulnerability assessment in all areas that foreign nationals will reside or visit prior to a foreign national entering the facility. These OPSEC vulnerability assessments are not necessarily formal assessments but walk-through reviews by the OPSEC PM and other organizational personnel to determine what the visitor might see that would identify vulnerabilities. They must be completed in time to correct or change items that need it prior to the arrival of the foreign national(s).

3.2.1. AFMC Product, Logistics, Test Center, and site OPSEC PMs develop and monitor OPSEC education programs for their activity with the assistance of the AFMC OPSEC PM. Maximize the use of the Interagency OPSEC Support Staff (IOSS) computer based, in residence, and mobile training team classes, website (www.IOSS.gov), posters, and other products to enhance OPSEC awareness/education programs.

3.2.4. AFMC Product, Logistics, Test Center, installation, and site OPSEC PMs must successfully complete the Air Force OPSEC Program Manager's Course. Contact HQ AFMC/SFXP for training allocations. Completion of the IOSS 380 OPSEC course in-residence will satisfy this requirement. Courses are unit funded.

3.2.5. (Added) All AFMC military, civilian, and contractor personnel are responsible for understanding the OPSEC concept and the intelligence threat to AFMC operations and resources. Each must apply this understanding to their assigned duties.

3.4. Submit requests for interpretation or clarification of policy through OPSEC PM channels to HQ AFMC/SFXP.

3.6. Center and site OPSEC PMs submit annual reports to HQ AFMC/SFXP by 15 November of each calendar year. See AFI 10-1101, Attachment 6, for format.

3.7. (Added) Program Nickname.. The Air Force Materiel Command OPSEC program nickname is CORAL DRAGON, symbolic of the original OPSEC survey, PURPLE DRAGON, conducted during the Vietnam era. Use the purple winged dragon or variations for training purposes and program awareness initiatives.

4.1. AFMC organizations at AFMC centers or sites will participate in the center or site OPSEC program. AFMC organizations located on another MAJCOM's installation will participate in the host's OPSEC program. If the host has no OPSEC program, the tenant will participate in the AFMC program.

4.1.2. Organizational placement of the OPR at AFMC field activities is at the commander's discretion. However, commanders should consider co-locating the OPR with program protection or force protection personnel to ensure effective implementation across organizational and functional lines.

4.1.3. OPSEC PMs at all levels must have full knowledge and understanding of the operations and activities of their organizations. The OPSEC PM must have a close working relationship with personnel responsible for plans and operations within the organization. Together they determine the sensitivity of each plan or operation and identify operational vulnerabilities. Vulnerabilities should be eliminated if possible, or reduced by acceptable compensatory measures. When neither elimination nor reduction is possible or practical, conduct a risk assessment to evaluate the consequences of continuing the plan or operation.

4.1.5.1. (Added) AFMC Product, Logistics, Test Center, and site OPSEC PMs coordinate the OPSEC program within their organization and ensure subordinate units/elements within their oversight have viable OPSEC programs. OPSEC PMs perform staff assistance visits to subordinate elements at least annually, providing advice, assistance, and support. They perform OPSEC assessments on their own initiative (with the concurrence of the commander, director, manager of the surveyed elements), when requested by unit commanders/directors, or as directed by higher headquarters.

4.2.4. (Added) All AFMC Product, Logistics, and Test Centers, and AFMC sites will designate a primary and alternate OPSEC PM in writing. Send letters of appointment to HQ AFMC/SF; update appointment letters as changes occur. Appointment letters will include:

- Name
- Rank or Grade
- Security Clearance
- DSN/Commercial Telephone Number
- STU III or STE Number
- FAX Number/Secure FAX Number
- E-Mail address
- Mailing Address
- Office Symbol and Duty Title

4.2.4.1. (Added) All subordinate two-letter organizations or units will designate a primary and alternate OPSEC PM in writing. Send the letter of appointment to the center or site OPSEC PM. Update appointment letters as changes occur. Include the same information as required in paragraph 4.2.4 above.

4.3. OPSEC PMs at all levels must review the OPSEC annex in operations, wartime, contingency, and exercise plans that impact their organization at least annually. The OPSEC annex for each plan must include a list of CI applicable to the operation.

4.3.2. AFMC Centers and sites will have a written OPSEC Plan. An OPSEC plan can be a separate plan, an annex to a larger plan, or the integration of OPSEC into an overall mission or program protection plan.

OPSEC Plans will be reviewed/updated by the OPSEC PM annually for OPSEC currency. The OPSEC Plan will include the following:

- References
- General Mission/Program Description
- Security Responsibilities
- Critical Information list
- Indicators
- Threat
- Vulnerabilities
- Countermeasures
- Public Affairs
- Training
- Supporting Units/Associated Programs

4.4. The target group for this training is all military, civilian, and resident contractor personnel.

4.5. Units will provide adequate funding for OPSEC program manager training and OPSEC assessment/ survey costs. AFMC Center and site PMs will submit annual OPSEC course projections to HQ AFMC/ SFXP.

4.6.1. Document survey actions in writing and maintain copies with OPSEC records. Organizational/unit OPSEC PMs that require assistance in conducting OPSEC surveys should contact the center or site OPSEC PM.

4.6.1.1. (Added) AFMC Center and site OPSEC PMs conduct OPSEC surveys of selected programs and operations. Give particular attention to support of program planning for acquisition programs. OPSEC is a commander's program, hence; AFMC Centers, and sites will request OPSEC Multi-discipline Vulnerability Assessments (OMDVA) through HQ AFMC/SFXP who will coordinate with AFIWC for the assessment. OMDVAs should be requested at least every five years. HQ AFMC/SFXP will conduct SAVs at least once every three years.

A2.4.10. The OPSEC PM for AFMC resides in HQ AFMC/SF per authority of HQ USAF/XOXT, "Letter of Deviation," 9 February 1995.

Attachment 4.21. (Added) In addition to PM duties listed, AFMC Product, Logistics, Test Center, and site PM duties include, but are not limited to:

- Identifying OPSEC PMs at unit levels as required.
- Establishing an OPSEC working group as a staff forum for addressing command and local OPSEC policies, programs, and objectives. The working group must convene at least semi-annually. Send copies of working group minutes to HQ AFMC/SFXP.
- Coordinating with local protective security functions and AFOSI to ensure adequate funding for security countermeasures as determined necessary by OPSEC assessments.
- Ensuring OPSEC reviews are conducted on all organizational/unit web pages annually IAW AFI 10-1101, attachment 4, paragraph 5.

- Ensuring vulnerability assessments are conducted on all areas where foreign nationals are housed or visit prior to their arrival within the organization.
- Establishing and maintaining a comprehensive continuity file.
- Supplementing this publication as necessary. Notifying HQ AFMC/SFXP when supplement is published.

A.4.22. (Added) HQ AFMC/SF is the OPR for Military Deception (MD), formerly known as Tactical Deception (TD). Coordinate MD operations with this office. The OPSEC OPR for AFMC centers, site, and subordinate organizations will be the MD focal point.

LEROY L. WALTERS, Col, USAF
Director, Security Forces